REMARKS

No claims have been cancelled or added. Claim 30 has been amended. Claims 1-48 are currently pending in the application. In view of the following remarks, Applicant respectfully requests withdrawal of the rejections and forwarding of the application onto issuance.

Objection to Drawings

The Office objects to Fig. 2 due to a missing reference numeral. The Office also points out that the box entitled Process Manager 60c is referenced in the specification as 60b. Applicant thanks the Office for its attention to detail and herewith submits a corrected Fig. 2.

The § 102 Rejections

Claims 1-10 and 25-48 stand rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,757,919 to Herbert et al (hereinafter "Herbert").

The § 103 Rejections

Claims 11-18 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Herbert in view of U.S. Patent No. 5,628,023 to Bryant et al. (hereinafter "Bryant").

Claims 19-24 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Herbert in view of U.S. Patent No. 6,003,117 to Buer et al. (hereinafter "Buer").

Applicant's Disclosure

Before Applicant specifically addresses the Office's rejections, the following discussion is provided to assist the Office in appreciating the patentable distinctions between Applicant's claimed embodiments and the cited references.

One of the problems that continues to confront traditional paging operating systems concerns the treatment of sensitive information (e.g. passwords to access network resources, credit card information used during an Internet shopping session, and the like). For example, when an individual, using a password, logs onto an operating system such as Windows NT, the individual's password can typically be kept in memory for various reasons. For example, if the user locks a work station and wants to later unlock it, the operating system needs to validate against something. Thus, the operating system goes out to main memory and compares what is typed in by a user with what is sitting in the memory. Between these two points in time, however, the password may have entered the paging file because the operating system may have decided that the logon process was idle. Having the password in the paging file can leave it open to attack, e.g. if the machine on which the paging file is located were to be physically stolen. Thus, because of the nature of paging operating systems, sensitive information can sometimes be undesirably placed in a paging file in secondary memory. In security-sensitive installations, preventing the sensitive information from reaching the paging file may be advantageous.

Applicant provides methods and systems to protect unencrypted sensitive information from being paged out to secondary memory, such as a hard disk, during paging operations. In various embodiment described in Applicant's specification, a key is provided and is maintained in the main memory of a virtual memory system. Measures are taken to protect the key such as ***page-locking the***

key in the main memory to ensure that it ***never gets paged out*** to the secondary memory. This aspect, combined with the nature of the key (i.e. a very large random key) provides a degree of protection that previously was not afforded. For example, if the key cannot be paged out to the paging file, then it is not susceptible to capture.

The Herbert Reference

In contrast, Herbert teaches a method and system for maintaining integrity and confidentiality of pages ***paged to an external storage unit*** from a physically secure environment. An outgoing page is selected to be exported from a physically secure environment to an insecure environment. An integrity check value is generated and stored for the outgoing page. In one embodiment, this takes the form of taking a one-way hash of the page using a well-known one-way hash function. The outgoing page is then encrypted. Herbert teaches key generation using a random number generator. However, there is *no teaching or suggestion* to ***page-lock the key*** or ***store the key in a non-pageable page***.

Claims 1-10

Claim 1 recites, in a paging operating system having physical memory for holding information and secondary storage comprising a page file for receiving information that is paged out from the physical memory, a computer-implemented method of protecting information comprising [emphasis added]:

- encrypting information using a ***key that is page-locked in the physical memory***; and
- paging out, to the page file, the encrypted information.

In making out the rejection of this claim, the Office argues that Herbert teaches a method for encrypting information using a key in the physical memory and paging out the encrypted information. Applicant agrees that Herbert teaches a method of encrypting information using a key. Applicant also agrees that Herbert teaches paging out the encrypted information. However, Applicant traverses the rejection of this claim because, as noted above, Herbert ***does not teach*** encrypting information using a ***key that is page-locked in the physical memory***. The Office cites to column 1, lines 65-67, and column 2, lines 2-3, of Herbert in support of its argument that Herbert anticipates the subject matter of this claim. Those excerpts are reproduced below:

> The outgoing page is then encrypted using a cryptographically strong encryption algorithm. *Col. 1, lines 65-67.*
>
> The encrypted outgoing page is then exported to the external storage. *Col. 2, lines 2-3.*

Neither of these excerpts even *suggests* encrypting information using a key that is ***page-locked*** in the physical memory. Accordingly, for at least this reason, this claim is allowable.

Claims 2-10 depend either directly or indirectly from claim 1 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 1, are neither disclosed nor suggested by the references of record either singly or in combination with one another.

Claims 11-18

Claim 11 recites, in a paging operating system having main memory for holding information and secondary storage comprising a page file for receiving information that is paged out from the main memory, a computer-implemented method of protecting information comprising [emphasis added]:

- ***page-locking a key*** in main memory;
- restricting access to the ***page-locked key*** to only the operating system kernel;
- calling the operating system kernel to encrypt information;
- accessing the ***page-locked key*** with the operating system kernel; and
- using the operating system kernel to encrypt the information with the ***page-locked key***.

In making out the rejection of this claim, the Office argues that the combination of Herbert and Bryant render the claimed subject matter obvious. Applicant strongly disagrees and traverses the rejection. In making out its rejection, the Office argues that Herbert discloses a method for page-locking a key in main memory. In support of its argument, the Office cites to column 5, lines 59-67, which is reproduced below in its entirety:

> In one embodiment, the active pages will represent a page table and one or more page frames for each piece of software. For example, software 140 has page table 141 and page frames 142-144 residing in secure memory. Similarly, software 160 and 170 have page tables 161, 171 and page frames 162, 172, respectively, active in the secure RAM. Conversely, software 150 has its page table and all its page frames paged out to the external storage unit 4.

Applicant respectfully submits that, not only does the cited excerpt ***not teach*** encrypting information using a key that is ***page-locked*** in the physical memory, the cited excerpt does not even *mention* a key. As noted above, Herbert does make use of a randomly-generated key, but there is no teaching or suggestion that the key is ***page-locked*** in the physical memory. In addition, the cited sections of Bryant do not provide this missing feature.

Accordingly, for at least this reason, this claim is allowable.

Claims 12-18 depend either directly or indirectly from claim 11 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 11, are neither disclosed nor suggested by the references of record either singly or in combination with one another.

<u>**Claims 19-24**</u>

Claim 19 recites, in a paging operating system having main memory for holding information and secondary storage comprising a page file for receiving information that is paged out from the main memory, a computer-implemented method of handling encrypted information comprising [emphasis added]:

- accessing encrypted information in the page file; and
- decrypting the encrypted information with a ***key that is page-locked in the main memory***.

In making out the rejection of this claim, the Office states that Herbert does not disclose a method for decrypting the encrypted information with a key that is page-locked in the main memory. Applicant agrees. The Office then argues that Buer supplies the missing feature. Applicant strongly disagrees and traverses the rejection. In support of its argument, the Office cites to column 2, lines 27-36, of Buer, which is reproduced below in its entirety:

> In the preferred embodiment, the processor uses an encryption engine which to decrypt the first data and encrypt the second data. For example, the encryption engine performs a DES encrypt operation to decrypt the first data. Likewise, the encryption engine performs a DES decrypt operation to encrypt the second data. Alternatively, other encryption/decryption algorithms may be used.
>
> Also in the preferred embodiment, a memory controller is

used to access unencrypted data stored in the external memory.

Applicant respectfully submits that, not only does the cited excerpt ***not teach*** decrypting the encrypted information with a key that is ***page-locked*** in the main memory, this excerpt does not even *mention* the key. As such, there is no teaching or suggestion of a key is ***page-locked*** in the main memory.

Accordingly, for at least this reason, this claim is allowable.

Claims 20-24 depend either directly or indirectly from claim 19 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 19, are neither disclosed nor suggested by the references of record either singly or in combination with one another.

Claims 25-29

Claim 25 recites, in a paging operating system having main memory for holding information and secondary storage comprising a page file for receiving information that is paged out from the main memory, a computer-implemented method of protecting information comprising [emphasis added]:

- allocating a non-pageable page of main memory;
- generating a random key; and
- ***storing the random key in the non-pageable page of main memory***, the random key being configured for use by the operating system to encrypt information that might be paged out to the page file.

In making out the rejection of this claim, the Office argues that Herbert anticipates the subject matter of this claim. Applicant strongly disagrees and traverses the rejection. In making out its rejection, the Office apparently cites to column 2, lines 2-3, to support its argument that Herbert teaches storing a random key in a non-pageable page of main memory. The cited excerpt is reproduced below:

> The encrypted outgoing page is then exported to the external storage.

Applicant respectfully submits that, not only does the cited excerpt ***not teach*** storing a random key in a ***non-pageable*** page of main memory, the excerpt does not even *mention* a key. As noted above, Herbert does make use of randomly-generated key, but there is no teaching or suggestion that the key is stored in a ***non-pageable*** page of main memory.

Accordingly, for at least this reason, this claim is allowable.

Claims 26-29 depend either directly or indirectly from claim 25 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 25, are neither disclosed nor suggested by the references of record either singly or in combination with one another.

Claims 30-35

As amended, **claim 30** recites, in an operating system having main memory for holding information and secondary storage for receiving information that is transferred out of main memory, a computer-implemented method of protecting information comprising [emphasis added]:

- generating at least one ***non-pageable random key*** by using a random key generation process;
- encrypting at least one selected block of information in the main memory with a software component that uses the at least one random key for encryption;
- transferring the one encrypted block of information to the secondary storage;

- decrypting the one encrypted block of information with the software component that uses the at least one random key for decryption; and
- placing the decrypted block of information in the main memory.

In making out the rejection of this claim, the Office argues that Herbert anticipates the subject matter of this claim. Applicant strongly disagrees and traverses the rejection. In making out its rejection, the Office cites to column 2, lines 63-67, and column 3, lines 1-5, to support its argument. That excerpt is reproduced below in its entirety:

> An encryption/decryption engine 12 encrypts outgoing pages and decrypts incoming pages at the interface before sending them to the external storage 4 or integrity check engine 13, respectively, thereby providing a confidentiality service. A random number generator 18 is coupled to bus 17 to generate keying material for the encryption engine 12. An incoming page is decrypted by encryption engine 12 and passed to the integrity check engine 13 which calculates a one-way hash value of the incoming page.

Applicant respectfully submits that, not only does the cited excerpt ***not teach*** generating at least one ***non-pageable random key***, the excerpt does not even *mention* a key. As noted above, Herbert does make use of a randomly-generated key, but there is no teaching or suggestion to generate at least one ***non-pageable*** key by using a random key generation process.

Accordingly, for at least this reason, this claim is allowable.

Claims 31-35 depend either directly or indirectly from claim 30 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 30, are neither disclosed nor suggested by the references of record either singly or in combination with one another.

__Claims 36-40__

Claim 36 recites a system for use in protecting pageable information comprising [emphasis added]:

- a memory having pageable and non-pageable pages; and
- at least one ***key stored in the memory in a non-pageable page***, the key being configured for use in encrypting pageable information.

In making out the rejection of this claim, the Office argues that Herbert anticipates the subject matter of this claim. Applicant strongly disagrees and traverses the rejection. In making out its rejection, the Office cites to column 5, lines 26-29, to support its argument. That excerpt is reproduced below:

> One embodiment of the invention employs a paging hierarchy in which the page directory always resides in the secure RAM 14 and a page table is associated with each application.

Applicant respectfully submits that, not only does the cited excerpt ***not teach*** at least one ***key stored in the memory in a non-pageable page***, the excerpt does not even *mention* a key. As noted above, Herbert does make use of randomly-generated key, but there is no teaching or suggestion to store at least one key in the memory in a ***non-pageable*** page.

Accordingly, for at least this reason, this claim is allowable.

Claims 37-40 depend either directly or indirectly from claim 36 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 36, are neither disclosed nor suggested by the references of record either singly or in combination with one another.

Claim 41

Claim 41 recites a computer program embodied on one or more computer-readable media, the program comprising [emphasis added]:

- encrypting information with a ***key that is page-locked in main memory*** of a computer;
- paging out, to secondary storage, the encrypted information;
- accessing the encrypted information in the secondary storage; and
- decrypting the encrypted information with the ***key that is page-locked in the main memory***.

In making out the rejection of this claim, the Office argues that Herbert discloses encrypting information with a key that is page-locked in main memory. Applicant strongly disagrees and traverses the rejection of this claim because, as noted above, Herbert ***does not teach*** encrypting information with a ***key that is page-locked in main memory***. The Office cites to column 1, lines 65-67, and column 2, lines 2-3, of Herbert in support of its argument. Those excerpts are reproduced below:

> The outgoing page is then encrypted using a cryptographically strong encryption algorithm. *Col. 1, lines 65-67.*
>
> The encrypted outgoing page is then exported to the external storage. *Col. 2, lines 2-3.*

Neither of the cited excerpts even *suggests* encrypting information with a key that is ***page-locked*** in main memory. Accordingly, for at least this reason, this claim is allowable.

Claims 42-46

Claim 42 recites a programmable computer comprising [emphasis added]:

- a processor;
- main memory for holding information;
- secondary storage for receiving information that is temporarily transferred out of the main memory;
- the computer being programmed with computer-readable instructions which, when executed by the processor, cause the computer to:
    - encrypt information that is to be transferred to the secondary storage ***with a key that is locked in the main memory***;
    - transfer the encrypted information to the secondary storage; and
    - decrypt the encrypted information with a key that is locked in the main memory.

In making out the rejection of this claim, the Office argues that Herbert discloses encrypting information with a key that is page-locked in main memory. Applicant strongly disagrees and traverses the rejection of this claim because, as noted above, Herbert ***does not teach*** encrypting information that is to be transferred to the secondary storage with a ***key that is locked in the main memory***. The Office cites to column 1, lines 65-67, and column 2, lines 2-3, of Herbert in support of its argument. Those excerpts are reproduced below:

> The outgoing page is then encrypted using a cryptographically strong encryption algorithm. *Col. 1, lines 65-67.*
>
> The encrypted outgoing page is then exported to the external storage. *Col. 2, lines 2-3.*

Neither of the cited excerpts even *suggests* encrypting information that is to be transferred to the secondary storage with a key that is ***locked*** in the main memory. Accordingly, for at least this reason, this claim is allowable.

Claims 43-46 depend either directly or indirectly from claim 42 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 42, are neither disclosed nor suggested by the references of record either singly or in combination with one another.

__Claim 47__

Claim 47 recites one or more application programming interfaces embodied on one or more computer-readable media for execution on a computer in conjunction with a paging operating system having main memory for holding information and a page file for receiving information that is paged out from the main memory, comprising [emphasis added]:

- an interface method for encrypting pageable information with a ***key that is page-locked in the main memory***; and
- an interface method for decrypting encrypted information that is contained in the page file.

In making out the rejection of this claim, the Office argues that Herbert anticipates this claim. Applicant strongly disagrees and traverses the rejection of this claim because, as noted above, Herbert ***does not teach*** an interface method for encrypting pageable information with a ***key that is page-locked in the main memory***. The Office cites to column 2, lines 63-67, of Herbert in support of its argument. That excerpt is reproduced below:

> An encryption/decryption engine 12 encrypts outgoing pages and decrypts incoming pages at the interface before sending them to the external storage 4 or integrity check engine 13, respectively, thereby providing a confidentiality service.

The cited excerpt does not even *suggest* an interface method for encrypting pageable information with a key that is ***page-locked*** in the main memory. Accordingly, for at least this reason, this claim is allowable.

Claim 48

Claim 48 recites an application programming interface embodied on a computer-readable medium for execution on a computer in conjunction with a paging operating system having main memory for holding information and secondary storage comprising a page file for receiving information that is paged out from the main memory, comprising a method for setting an attribute on a page of main memory, the attribute designating that the page must be encrypted with a ***key that is page-locked in the main memory*** prior to the page being paged out to the page file.

In making out the rejection of this claim, the Office argues that Herbert anticipates this claim. Applicant strongly disagrees and traverses the rejection of this claim because, as noted above, Herbert ***does not teach*** a method for setting an attribute on a page of main memory in which the attribute designates that the page must be encrypted with a ***key that is page-locked in the main memory*** prior to the page being paged out to the page file. The Office cites to column 1, lines 60-63, and column 3, lines 13-15, in support of its argument. Those excerpts are reproduced below:

> An outgoing page is selected to be exported from a physically secure environment to an insecure environment. An integrity check value is generated and stored for the outgoing page. *Col. 1, lines 60-63.*
>
> But, it is within the scope and contemplation of the invention that either or both engines may be implemented as software. *Col. 3, lines 13-15.*

The cited excerpt does not even *suggest* a method for setting an attribute on a page of main memory, the attribute designating that the page must be encrypted with a key that is ***page-locked*** in the main memory prior to the page being paged out to the page file.

Accordingly, for at least this reason, this claim is allowable.

Conclusion

All of the claims are in condition for allowance. Accordingly, Applicant requests that a Notice of Allowability be issued forthwith. If the Office's next anticipated action is to be anything other than issuance of a Notice of Allowability, Applicant requests that the undersigned be contacted for the purpose of scheduling an interview.

Respectfully submitted,

Dated: 3/24/04

By: ________________________
Lance R. Sadler
Reg. No. 38,605
(509) 324-9256 ext. 226